

EXHIBIT 6



EDÖB-A-C0633401/2

Memorandum

dated 25 June 2021

concerning

**Swiss Firm Data Processing and Sharing of Information
with the U.S. Securities and Exchange Commission**



Table of Contents

1. Introduction	3
1.1 Starting Point	3
1.2 Summary of SEC Examination Authority and Process	3
1.3 Relevant Legal Basis	5
2. Legal Analysis	5
2.1 Applicability of the FADP	5
2.2 Cross-border Disclosure: Introduction	6
2.3 Cross-border Transfers based on Art. 42c para. 1 FINMASA	7
2.3.1 Introduction	7
2.3.2 Preservation of the Principle of Specialty and Confidentiality	7
2.3.3 Preservation of the Rights of the Clients and Third Parties	8
2.4 Cross-border Transfers under Art. 6 para. 2 FADP	8
2.4.1 General Comments	8
2.4.2 Consent	9
2.4.3 Contract	10
2.4.4 Data Processing in the Context of an Employment Relationship	12
2.4.5 Overriding Public Interest	12
2.4.6 Conclusion regarding Art. 6 para. 2 FADP	13
2.5 Data Protection Principles	14
2.5.1 General Comments	14
2.5.2 Evidence of the Collection of Personal Data	14
2.6 Breach of Professional Confidentiality	15
2.7 Conclusions	16



1. Introduction

1.1 Starting Point

On 22 December 2020 the Federal Data Protection and Information Commissioner (FDPIC) was contacted by the U.S. Securities and Exchange Commission (SEC) and asked whether the FDPIC could provide guidance with regard to the question if and how Swiss-domiciled entities registered with the SEC may transfer books and records containing personal data to the SEC as part of the SEC's inspection and examination program. More precisely, the SEC would like to know whether and – if yes – under which conditions Swiss data protection law permits a cross-border transfer of personal data to the SEC in the course of an examination process conducted by this authority. The FDPIC offered to answer this question in the form of a short memorandum for the attention of the SEC. On 9 February 2021 the SEC provided the FDPIC with a "Summary of SEC Examination Authority and Process". The findings of this summary (see below 1.2) form the basis for the subsequent legal analysis (see below 2.). On 31 May 2021, the FDPIC delivered a first version of the memorandum. This version dated 25 June 2021 is the final one.

This memorandum reflects the FDPIC's view of the relevant aspects of Swiss data protection. As the FDPIC is only competent to interpret Swiss data protection law, it cannot be discussed whether or under which conditions a transfer of personal data to the SEC is compatible with other Swiss laws. In particular, it must be left open whether or under which conditions criminal law allows the transfer of personal data covered by the protection of secrets under criminal law¹. Finally, but the Swiss courts are competent to decide in a legally binding way about the interpretation of Swiss data protection law.

1.2 Summary of SEC Examination Authority and Process

In its "Summary of the SEC Examination Authority and Process" the SEC states as follows:

"Pursuant to the U.S. law, certain firms must retain certain books and records and provide them directly to the U.S. Securities and Exchange Commission ("SEC") upon request. These firms include Swiss-based firms or branches that are registered, required to be registered, or otherwise regulated by the SEC as investment advisers, broker-dealers, clearing agencies, and transfer agents. The universe of Swiss-based registrants currently includes 66 investment advisers, 1 broker-dealer, and 7 broker-dealer branch offices. There are 10 Swiss-based investment advisers with pending applications for SEC registration. The SEC also expects 2 Swiss-based security-based swap dealers to register by the end of 2021. The SEC may also request information from Swiss-based entities that are not registered with the SEC, including audit firms, in furtherance of examinations of SEC registrants or in other limited circumstances.

Examples of relevant U.S. laws include Section 204 of the Investment Advisers Act of 1940 ("Advisers Act"), which gives the SEC the authority to request and examine the books and records of an SEC regulated investment adviser. Section 17 of the Securities Exchange Act of 1934 ("Exchange Act") provides the same authority in connection with SEC registered broker-dealers, clearing agencies, transfer agents, and other types of SEC regulated entities. Various rules, including Rule 204-2 of the Advisers Act and Rule 17a-4 of the Exchange Act, require firms to make and keep certain records and provide copies thereof to SEC staff upon request.

As part of the examination process, SEC staff typically sends the entity a letter notifying it of the examination and containing an initial request list that identifies certain information or documents that SEC staff will review as part of the examination. As the examination progresses, staff sends the entity additional requests for information and documents, as needed. U.S. securities laws re-

¹ Namely bank-client and business confidentiality.



quire entities to provide requested documents promptly to SEC staff, unredacted. In practice and as a courtesy, SEC staff asks that entities provide requested documents, including those containing personal data, no later than two weeks from the date of the request. SEC staff requests these books, records, and other materials to evaluate compliance with U.S. legal obligations and to prevent and/or enforce against potential illegal behavior. Failure to provide information promptly as requested would generally violate the firm's regulatory requirements, would be deemed to be impeding an examination, and might result in an enforcement referral or, if severe, an enforcement action.

The SEC does not conduct routine or cycle examinations. Instead, the SEC uses a risk-based approach to selecting examination candidates and scope areas for each examination. For example, SEC staff examines approximately 15 percent of all (domestic and international) SEC registered investment advisers (RIAs) each year. The selection of firms to examine is based on a risk-based assessment. SEC staff considers a number of potential risk factors, such as, among others, products and services offered, prior examination observations and conduct, disciplinary history of associated individuals or affiliates, changes in leadership or other personnel, and, in the context of RIAs, whether a RIA has access to investor assets. As a result, the determination of whether to examine a firm is evaluated year to year. Once SEC staff selects a firm for examination, we conduct an additional risk assessment at the firm level to determine the scope of the examination (that is, selecting particular areas of the business for review). Therefore, aside from certain requests for background information (e.g., organizational charts) that are standard requests in each exam, the scope of the examination (and consequently the documents requested) varies from firm to firm depending on the firm's business model and associated risks.

Depending on the scope of the particular examination of an entity, information requested during an examination focuses on a wide range of information, including office policies, procedures, organizational charts, employee lists, director details, board meeting minutes, employee disciplinary history, employment applications/questionnaires, employee personal trading records, financial transaction records, customer complaints, customer agreements, internal communications, and documents relating to service providers such as consultants and auditors (see Attachment A for some examples of SEC staff requests). Many of these records include personal data, which is needed to assess compliance with a number of requirements under the U.S. securities laws. It is the SEC's practice to limit the type and amount of personal data it requests during examinations to targeted requests based on risk and related to specific clients and accounts, and employees. That said, some degree of personal data of employees and clients (both individual and institutional) regardless of their physical location or nationality is crucial to assessing compliance with many obligations under the U.S. laws, such as the existence of conflicts of interest and whether clients are treated fairly. The requested information may include follow-up requests regarding some limited administrative or criminal proceedings and sanctions information that constitute "sensitive personal data" under the Swiss Federal Act on Data Protection that have already been reported to the SEC as part of the registration and reporting regimes.

SEC examinations are non-public. Information, data, and documents received by the SEC are maintained in a secure manner and, under strict US laws of confidentiality. Information about individuals cannot be onward shared save for certain uses publicly disclosed by the SEC, including in an enforcement proceeding, pursuant to a lawful request of the U.S. Congress or a properly issued subpoena, or to other regulators who have demonstrated a need for the information and provide assurances of confidentiality. Information from SEC examinations is also subject to provisions of the U.S. Freedom of Information Act that protect confidential information. The SEC uses what it obtains solely for its own lawful, regulatory purpose and is subject to audit by the US Government Accountability Office and other governmental oversight."



1.3 Relevant Legal Basis

The relevant Swiss legal bases are the Federal Act on Data Protection of 19 June 1992 (FADP; CC 235.1), the Ordinance to the Federal Act of Data Protection of 14 June 1993 (DPO; CC 235.11), the Federal Act on the Swiss Financial Market Supervisory Authority of 22 June 2007 (FINMASA; CC 956.1), as far as it refers to aspects of data protection, as well as Switzerland's Federal Code on Private International Law of 18 December 1987 (CPIL; CC 291).

The current FADP was recently subject to a total revision; it is foreseen that the revised version – the Federal Data Protection Act of 25 September 2020 (Revised FADP; published in the Swiss Federal Gazette 2020, p. 7639 ss.) – will come into force in the course of 2022. In the context of this memorandum, the legal situation under the Revised FADP will be considered where necessary.

As explained further below, there are situations where the General Data Protection Regulation (GDPR) applies, even though the company processing the data is domiciled in Switzerland (see below 2.1). However, this memorandum focuses on Swiss law and does not consider the GDPR, the interpretation of which is primarily a task of the competent data protection authorities and courts in the EU.

2. Legal Analysis

2.1 Applicability of the FADP

The FADP applies to the processing of personal data pertaining to natural persons and legal persons (see Art. 2 para. 1 FADP). The Revised FADP applies – as the GDPR – but to the processing of personal data pertaining to natural persons (see Art. 1 Revised FADP). Personal data is all information relating to an identified or identifiable person (see Art. 3 let. a FADP). Processing means any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data (see Art. 3 let. e FADP).

If a firm is domiciled in Switzerland and processes personal data in Switzerland, infringements of personality rights resulting from the processing of personal data are governed, at the option of the injured party, by the FADP even if the person whose data is processed (the data subject) is domiciled abroad (see Art. 139 para. 3 and para. 1 let. b CPIL). Consequently, the FADP can also apply if a Swiss-domiciled entity processes personal data of U.S. residents or EU residents. Furthermore, if a controller or processor established in Switzerland processes personal data of natural persons who are in the EU, there are certain situations where the GDPR applies (see Art. 3 para. 2 GDPR).

In certain cases, the FADP does not apply, even though personal data are processed (see Art. 2 para. 2 FADP). It does, in particular, not apply in the case of one of the following pending proceedings (see Art. 2 para. 2 let. c FADP): pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or under administrative law (with the exception of administrative proceedings of first instance). The idea of the legislator was that, in these situations, the relevant procedural law assures data protection. In cases where Swiss-domiciled entities are required to transfer personal data to the SEC as part of the SEC's examination program, there are no pending proceeding in the sense of Art. 2 para. 2 let. c FADP². There are not any other reasons excluding the application of the FADP either. Consequently, the FADP applies.

² See Du PASQUIER/MENOUD, in: Watter et al. (eds.), Finanzmarktaufsichtsgesetz / Finanzmarktinfrakturgesetz, 3. ed., Basel 2019, Art. 42c N 30, regarding the transfer of information based on Art. 42c para. 1 FINMASA.



2.2 Cross-border Disclosure: Introduction

The cross-border disclosure of data is ruled by Art. 6 FADP. Disclosure means making personal data accessible, for example by permitting access, transmission or publication (see Art. 3 let. f FADP).

Under Swiss law, personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of a legislation that guarantees adequate protection (see Art. 6 para. 1 FADP). The FDPIC publishes a (non-binding) list of the states whose legislation ensures an adequate level of data protection (Art. 7 DPO)³. In his opinion, the U.S. legislation does not guarantee an adequate protection of the privacy as required by the FADP⁴.

According to the FADP, anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so (Art. 12 para. 1 FADP). If there is a data transfer to a country without a legislation that guarantees adequate data protection (see Art. 6 para. 1 FADP), the privacy of the data subject is, as a rule, unlawfully breached.

In general, a breach of privacy is unlawful unless it is justified by the consent of the injured party, by an overriding private or public interest or by law (see Art. 13 para. 1 FADP). With regard to data transfers to a country without a legislation guaranteeing an adequate data protection (see Art. 6 para. 1 FADP), the legislator has created a special rule: Such a data transfer is allowed but in one of the following special situations mentioned in Art. 6 para. 2 FADP:

- a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
- b. the data subject has consented in the specific case;
- c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
- d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
- f. the data subject has made the data generally accessible and has not expressly prohibited its processing;
- g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

Private entities that want to disclose personal data to the SEC, must make sure that each envisaged disclosure meets the requirements of Art. 6 FADP. Otherwise, they risk to be liable for damages⁵. It is in their responsibility to make sure that Art. 6 FADP is observed, not in the responsibility of the SEC⁶.

³ See [Transborder data flows \(admin.ch\)](#).

⁴ See also the FDPIC's policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 para. 1 Swiss FADP, available under: [Transborder data flows \(admin.ch\)](#). Regarding the GDPR, see Court of Justice of the European Union, judgement C-311/18 "Facebook Ireland and Schrems" of 16 July 2020.

⁵ See MAURER-LAMBROU/STEINER, in: Maurer-Lambrou/Blechta (eds.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. ed., Basel 2014, Art. 6 N 13.

⁶ SEC employees that process personal data can only be held responsible under the FADP, if the FADP applies to the processing of data by them. Provided that the FADP applies under private international law, the scope of the FADP is limited to the processing of data by private persons or federal bodies (see Art. 2 sec. 1 FADP; also see Art. 2 sec. 1 Revised FADP). "Private persons" are those persons that process data in the context of a matter which is itself governed by private law. The FDPIC assumes that the SEC's supervisory activities are governed by foreign public law. Consequently, if and to the extent SEC employees act within the scope of their supervisory activities, they are not private individuals within the meaning of the FADP and the FADP does not apply.



Nonetheless, if there is a special legal basis in Swiss law (a legal basis outside the FADP) that permits a transfer of data to a country without an adequate level of data protection, data processors are not bound by Art. 6 FADP and may transfer the data under the specific conditions set up by the special legal basis. Whether such a special legal basis exists, is examined below (see below 2.3).

According to the Revised FADP, there is no unlawful breach of privacy (see Art. 30 para. 1 Revised FADP) if personal data are disclosed abroad and the Swiss Federal Council has determined that the legislation of the relevant State or international body guarantees an adequate level of protection (see Art. 16 para. 1 Revised FADP). In the absence of such a decision by the Federal Council, personal data may be disclosed abroad only if appropriate protection is guaranteed by certain legal instruments (e.g. an international treaty or data protection provisions of a contract, see Art. 16 para. 2) or in specific exceptions, e.g. with an explicit consent of the data subject (see Art. 17 para. 1 Revised FADP).

2.3 Cross-border Transfers based on Art. 42c para. 1 FINMASA

2.3.1 Introduction

Persons and entities that under the financial market acts require to be licensed, recognized, or registered by the Financial Market Supervisory Authority as well as collective capital investments are subject to financial market supervision and consequently to the Financial Market Supervision Act (see Art. 3 FINMASA). Financial market supervision has the objectives of protecting creditors, investors, and insured persons as well as ensuring the proper functioning of the financial market (Art. 4 FINMASA). The supervising authority is the Swiss Financial Market Supervisory Authority (FINMA) (Art. 5 FINMASA).

The cooperation with foreign bodies is ruled by the Art. 42 ss. FINMASA. Art. 42c FINMASA allows for the direct transmission of non-public information by supervised parties. According to Art. 42c para. 1 FINMASA, supervised parties – i.e. supervised persons and entities in the sense of Art. 3 FINMASA – may transmit non-public information to the foreign financial market supervisory authorities responsible for them and to other foreign entities responsible for supervision provided that

- a. the conditions set out in Art. 42 para. 2 FINMASA are fulfilled (see further below 2.3.2)
- b. and that the rights of clients and third parties are preserved (see further below 2.3.3).

Transmissions under Art. 42c FINMASA may be made spontaneously or in response to a request from a foreign authority or entity. Art. 42c FINMASA applies but when information is transmitted from Switzerland to another country⁷.

2.3.2 Preservation of the Principle of Specialty and Confidentiality

Art. 42 para. 2 FINMASA requires that the information received by the foreign financial market supervisory authority is used exclusively to implement financial market law, or is forwarded to other authorities, courts or bodies for this purpose (principle of specialty). Furthermore, the requesting authority is bound by official or professional secrecy, notwithstanding provisions on the public nature of proceedings and the notification of the general public about such proceedings (principle of confidentiality).

FINMA publishes a list of financial market supervisory authorities to which it has provided administrative assistance in the past⁸. The courts have additionally ruled that specific authorities on the list meet the conditions regarding the principles of specialty and confidentiality or met them in a specific case at

⁷ See FINMA, Circular 2017/6 Direct transmission, N 3 and 4.

⁸ See <https://www.finma.ch/en/supervision/cross-sector-issues/direktuebermittlung/>.



the time the decision was made⁹. If an authority appears on the list, supervised parties may assume that it meets the conditions regarding the above-mentioned principles of specialty and confidentiality¹⁰.

The SEC appears on this list, and the FINMA has recently confirmed that there are currently no indications that a transfer of non-public information to the SEC in the course of an examination process conducted by this authority would not be allowed based on Art. 42c para. 1 let. a FINMASA. However, according to Art. 42c para. 1 let. b FINMASA, such transfer is allowed but if the rights of clients and third parties are preserved. As far as this provision concerns aspects of Swiss data protection, the FDPIC is competent to interpret it.

2.3.3 Preservation of the Rights of the Clients and Third Parties

Art. 42c para. 1 let. b FINMASA requires that the rights of clients and third parties are preserved if non-public information is transmitted to a foreign financial market supervisory authority. "Clients" are the natural persons and legal entities FINMASA and the financial market law are intended to protect, namely creditors, investors and insured persons¹¹. In the literature, the view is expressed that the holder of the customer secret should be the "client"¹². "Third parties" are to be understood as all other natural persons and legal entities that are mentioned in the information to be transmitted or can be identified from it, including employees of supervised parties, authorized representatives and beneficial owners¹³.

As far as the rights of clients and third parties are concerned, the relevant FINMA circular states that supervised parties must, inter alia, preserve business and bank-client confidentiality, data protection and rights pertaining to employment relationships¹⁴. From the point of view of data protection, Art. 42c para. 1 FINMASA is consequently not a legal basis justifying a transfer of personal data to a country without an adequate level of data protection (see Art. 13 para. 1 FADP and above 2.2). It only recalls that a cross-border disclosure must be compatible with the FADP, namely with Art. 6 FADP. Private entities that are required to transfer personal data to the SEC based on Art. 42c para. 1 FINMASA therefore have to respect the conditions set up by Art. 6 para. 2 FADP (see below 2.4).

2.4 Cross-border Transfers under Art. 6 para. 2 FADP

2.4.1 General Comments

According to Art. 6 para. 2 let. a FADP personal data may be transmitted to a country without an adequate level of data protection if sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad.

The Swiss-U.S. Privacy Shield cannot be considered as a sufficient safeguard in the sense of Art. 6 para. 2 let. a FADP: First of all, it is not possible for authorities to be certified under the Swiss- or under the EU-U.S. Privacy Shield. Secondly, the Court of Justice of the European Union has rendered on 16 July 2020 the decision "Schrems II" according to which the EU-US Privacy Shield can no longer

⁹ Ibid, N 20.

¹⁰ Ibid, N 21.

¹¹ FINMA, Circular 2017/6 Direct transmission, N 16.

¹² See DU PASQUIER/MENOUD, in: Watter/Bahar (eds.), Basler Kommentar Finanzmarktaufsichtsgesetz/Finanzmarktinfrastukturgesetz, 3. ed., Basel 2019, Art. 42c N 31.

¹³ FINMA, Circular 2017/6 Direct transmission, N 17.

¹⁴ Ibid, N 30.



be considered as an “adequacy” mechanism to protect cross-border transfers of personal data to the USA. In the view of the FDPIC this is also the case for the Swiss-U.S. Privacy Shield¹⁵.

The FDPIC generally welcomes efforts to create a transfer tool in the sense of Art. 6 para. 2 let. a FADP. However, according to applicable Swiss law, the creation of such a tool is not mandatory if a disclosure of personal data can be justified by one of the other conditions mentioned in Art. 6 para. 2 FADP. In the present case, this could be the consent of the data subject in the specific case (let. b), a contract (let. c) or an overriding public interest (let. d) (see below 2.4.2 ss.).

2.4.2 Consent

In the absence of a legislation that guarantees adequate protection, personal data may be disclosed abroad if the data subject has consented in the specific case (Art. 6 para. 2 let. b FADP). If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information (“informed consent”). Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles (Art. 4 para. 5 FADP). According to the Revised FADP, the consent to a transfer of data to a country without an adequate level of data protection must always be given expressly (see Art. 17 para. 1 let. a Revised FADP). Provided that the data subject has been adequately informed, consent can be given by way of a single declaration of consent but, in principle, also by accepting general terms and conditions.

A data subject's consent must be given voluntarily (Art. 4 para. 5 FADP). In practice, the data subject often does not have a choice. According to the comments of the Swiss Federal Council regarding the draft of the current FADP, a consent is not invalid because of the mere fact that a data subject that does not give his or her consent is confronted with a disadvantage. A consent is but invalid if there is no connection between the disadvantage and the purpose of the data processor or if the disadvantage is disproportionate with regard to this purpose¹⁶. Similarly, Art. 7 (4) GDPR states that when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. If a customer consents to a processing purpose that is not necessary for the performance of the contract, such consent is not freely given in case that the denial of the consent would lead to the denial of services¹⁷.

In the present case, a firm subject to SEC supervision cannot offer its services to customers if it is not willing to transfer customer data required by SEC in the case of an examination process. Anyone operating in a foreign market must comply with the rules there¹⁸. Failure to provide information to the SEC would generally violate the firm's regulatory requirements, would be deemed to be impeding an examination, and might result in an enforcement referral or, if severe, in an enforcement action¹⁹.

¹⁵ See the FDPIC's policy paper on the transfer of personal data to the USA and other countries lacking an adequate level of data protection within the meaning of Art. 6 para. 1 Swiss FADP, available under: [Transborder data flows \(admin.ch\)](https://www.fdpic.admin.ch/transborder-data-flows).

¹⁶ Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung dated 19 February 2003, Swiss Federal Gazette 2003 p. 2101 ss., p. 2127; MAURER-LAMBROU/STEINER, in: Maurer-Lambrou/Blechte (eds.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. ed., Basel 2014, Art. 4 N 16f.

¹⁷ See EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020, N 25 ss., in particular N 33.

¹⁸ See Botschaft zum Finanzmarktinfrastukturgesetz (FinfraG) dated 3 September 2014, Swiss Federal Gazette 2014 p. 7483 ss., p. 7620.

¹⁹ Summary of SEC Examination Authority and Process; see above 1.2.



Therefore, if a customer that is informed about the fact that his data can be transferred to the SEC, gives his consent to such a data processing, such consent is voluntarily given and valid, even though the firm would not have been prepared to enter into a contract if the customer had not consented.

However, if and to the extent data processing is necessary for the performance of the contract, the data processor has, in general, an overriding private interest to process the data (see also Art. 13 para. 1 FADP) such that the consent of the data subject is not necessary. Furthermore, a given consent may be revoked at any time. Of course, should the data processing be necessary for the performance of the contract, the contract could be terminated after the revocation of consent. With regard to Swiss firms subject to SEC supervision, this would, however, mean that they could not transfer data of former customers to the SEC when required to do so. The question is whether a transfer of customer data to the SEC can be justified by contract (Art. 6 para. 2 let. c FADP; see below 2.4.3).

2.4.3 Contract

In the absence of a legislation that guarantees adequate data protection, personal data may be disclosed abroad if the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party (Art. 6 para. 2 let. c FADP). According to Art. 17 para. 1 let. b Revised FADP personal data may be disclosed abroad if the disclosure is directly connected with the conclusion or the performance of a contract 1. between the controller and the data subject, or 2. between the controller and its contracting partner in the interest of the data subject²⁰.

Art. 6 para. 2 let. c FADP applies but if personal data of a contractual party is processed. Customers of the firms supervised by the SEC are contractual parties to these firms.

Furthermore, data processing must be directly connected with the conclusion or the performance of a contract. This means, e.g., that data must be processed for the purpose of the conclusion or performance of the contract and not on the occasion of the conclusion or performance of a contract²¹. A processing of data in the sense of Art. 6 para. 2 let. c FADP need not be imperative for the conclusion or performance of the contract. However, it must be typical for the relevant contract or at least lie within the range of expectation of the contractual partner²². A typical example for such data processing is the checking of the creditworthiness of the contractual partner with a credit agency or the disclosure of data by travel companies to transport companies in the context of international transport services.

The question is whether a transfer of customer data to the SEC is directly connected with the performance of the relevant contract. From a strict point of view, such disclosure is not made for the purpose of the performance of the contract, but because the relevant firm has been required to disclose the customer data in the course of a SEC examination process. Nonetheless, the record-keeping, reporting and inspection obligations provided for by U.S. law are preconditions for the registration of a Swiss firm with the SEC and for rendering the relevant services. Failure to provide information to the SEC would generally violate the firm's regulatory requirements, would be deemed to be impeding an examination, and might result in an enforcement referral or, if severe, in an enforcement action²³. In Swiss doctrine, it is controversial whether an invocation of contract as a basis of justification is possible in case that the contract in question has been terminated. However, after the termination of the contract

²⁰ The GDPR provides for analogous provisions, see Art. 49 (1) (b) and (c).

²¹ See ROSENTHAL, in: Rosenthal/Jöri (eds.), Handkommentar zum Datenschutzgesetz, Zurich/Basel/Geneva 2008, Art. 13 N 39.

²² Ibid, Art. 13 N 39. Different: Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung dated 19 February 2003, Swiss Federal Gazette 2003 p. 2101 ss., p. 2129, according to which the processing must be imperative for the conclusion or performance of the contract.

²³ Summary of SEC Examination Authority and Process, see above 1.2.



the justification of contract is often of particular relevance because here the data processor must, in principle, have the possibility to process the data of his contractual partner even against his will and therefore without his consent²⁴. In the view of the FDPIC, a data processor has, in principle, a legitimate interest to transfer the data of his contractual partner to a foreign supervisory authority requiring the data, even after the termination of the contract. Consequently, a transfer of data of present or former customers to the SEC could be justified by Art. 6 para. 2 let. c FADP.

Art. 6 para. 2 let. c FADP does, however, not justify any transfer of data to any supervisory authority. Whether a justification exists, must be decided on the basis of the specific circumstances of the individual case by carefully weighing up the interests involved²⁵. Otherwise, there would be a risk that Swiss data protection law could be undermined by excessive foreign disclosure requirements. The starting point for weighing the interests of the data processor and the data subject can be whether the foreign provisions are comparable with analogous Swiss regulations and whether the foreign authorities to which the data is disclosed provide comparable protection of the confidentiality of the data as the Swiss authorities²⁶. The FINMA has powers over Swiss supervised entities comparable to those of the SEC²⁷. In order to implement the financial market acts, the FINMA may also itself carry out direct audits of supervised persons and entities abroad or have such audits carried out by audit agents (see Art. 43 para. 1. FINMASA). Furthermore, according to Art. 42c para. 1 let. a FINMASA, supervised parties may only transmit non-public information to the foreign financial market supervisory authorities responsible for them if the conditions set out in Art. 42 para. 2 FINMASA are fulfilled. This means, on the one hand, that the information is used exclusively to implement financial market law, or is forwarded to other authorities, courts or bodies for this purpose (Art. 42 para. 2 let. a). On the other hand, the requesting authorities have to be bound by official or professional secrecy, notwithstanding provisions on the public nature of proceedings and the notification of the general public about such proceedings (Art. 42 para. 2 let. b FINMASA)²⁸. As mentioned above, the SEC is listed on the list of financial market supervisory authorities to which the FINMA has provided administrative assistance. The supervised parties may therefore assume that the SEC meets the conditions mentioned in Art. 42 para. 2 FINMASA (see above 2.3.2). In view of the fact that the SEC complies with the requirements of Art. 42 para. 2 FINMASA, it can be assumed that the SEC provides sufficient protection of the confidentiality of the customer data and the supervised parties have therefore, in principle, an overriding private interest to disclose such data to the SEC if they have been required to do so (see Art. 13 para. 1 FADP). If the FINMA may provide administrative assistance and transmit personal data under these conditions, then it must, in principle, be possible for supervised parties to transmit personal data under the same conditions. Consequently, the transfer of customer data to the SEC can be based on Art. 6 para. 2 let. c FADP provided that, in the individual case, there are not any overwhelming interests of the data subject that do not allow the disclosure. It is the responsibility of the relevant Swiss firm to analyze whether there could be such overwhelming interests of the data subject and, in case of doubt, to obtain the consent of the relevant customer, if possible, or to refuse the disclosure, if necessary.

At this point, it is expressly left open how a disclosure of personal data that is protected by secrets under criminal law (in particular bank-client confidentiality) can be justified under criminal law, i.e. whether a consent is necessary or whether a disclosure can be justified otherwise. If criminal law requires consent, personal data may not be transferred to the SEC without such consent.

²⁴ See ROSENTHAL, in: Rosenthal/Jöhri (eds.), Handkommentar zum Datenschutzgesetz, Zurich/Basel/Geneva 2008, Art. 13 N 44.

²⁵ See RAMPINI, in: Maurer-Lambrou/Blechta (eds.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. ed., Basel 2014, Art. 13 N 26, regarding Art. 13 para. 2 FADP.

²⁶ Ibid, Art. 13 N 19, regarding Art. 13 para. 1 FADP.

²⁷ See in particular Art. 29 FINMASA.

²⁸ The reservation of Art. 42 para. 2 let. b FINMASA is necessary to take into account the rules of the U.S. Freedom of Information Act that require U.S. regulatory agencies to provide the public with regular notice in the media of proceedings that have been instituted and to publish the documents used to justify them (DU PASQUIER/MENOUD, in: Watter/Bahar (eds.), Basler Kommentar Finanzmarktaufsichtsgesetz/Finanzmarktinfrastukturgesetz, 3. ed., Basel 2019, Art. 42 N 86).



2.4.4 Data Processing in the Context of an Employment Relationship

Further above it was discussed whether consent (Art. 6 para. 2 let. b FADP) could be a possible legal basis for a cross-border disclosure (see above 2.4.2). However, a data subject's consent must be given voluntarily (see Art. 4 para. 5 FADP). The FDPIC assumes that if the disclosure of employee data to the SEC is provided for in the employment contract, the data subject cannot voluntarily consent to the data processing in question. Data subjects might, for certain reasons, be forced to work in the relevant business, and the consequence of not consenting to the data processing – i.e. the loss of a possibility to find a job with a SEC registered employer – is not tolerable for such persons. Consequently, data processing provided for in an employment contract, cannot be justified by consent.

The question arises whether a disclosure of employee data to the SEC can be based on another legal basis mentioned in Art. 6 para. 2 FADP. This presupposes first of all that the employer is allowed to process the relevant data about the employee. Art. 328b of the Swiss Code of Obligations (CO) states that the employer may handle data concerning the employee only to the extent that such data concern the employee's suitability for his job or are necessary for the performance of the employment contract.

Data necessary for the performance of the employment contract are all personal data concerning the employee, the processing of which is objectively necessary in order to fulfill a legitimate interest of the employer or employee in connection with the performance of the employment contract. On the one hand, this includes those data that an employer needs for the fulfillment of its legal and contractual obligations. Consequently, data disclosures to authorities within the scope of legal obligations of the employer are among those required for the performance of the employment contract²⁹. On the other hand, this includes all data that the employer needs to process in order to fulfill its own legitimate interests³⁰. This also includes, e.g., the defense against claims by third parties – including authorities – against the employer domestically or abroad which are based on facts in which the employee was or is involved within the framework of his employment relationship³¹. Legitimate interests of an employer in the processing of employee data may still exist after termination of an employment relationship³². In the opinion of the FDPIC, a disclosure of employee data to the SEC can be necessary for the performance of the employment contract, in which case data processing is compatible with Art. 328b CO.

If data in the sense of Art. 328b CO is disclosed abroad, Art. 6 FADP must be observed. In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad if the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party (Art. 6 para. 2 let. c FADP). This applies to all private contractual relationships, including those under labor law³³. On the basis of the foregoing, the FDPIC assumes that a transfer of employee data to the SEC is, in principle, justified by Art. 6 para. 2 let. c FADP. Nevertheless, it must be examined in each individual case whether there really is an overriding private interest of the data processor that justifies the disclosure (see above 2.4.3). Employee data may also be disclosed to the SEC if there is an overriding public interest (see Art. 6 para. 2 let. d FADP and below 2.4.5).

2.4.5 Overriding Public Interest

In the absence of a legislation that guarantees adequate protection, personal data may be disclosed abroad if disclosure is essential in the specific case in order to safeguard an overriding public interest

²⁹ EPINEY/CIMITELLA/ZBINDEN, *Datenschutzrecht in der Schweiz*, *Freiburger Schriften zum Europarecht* Nr. 10, 2009 (available under: [Microsoft Word - Cahier10 \(unifr.ch\)](#)), p. 35 and 36.

³⁰ ROSENTHAL, in: Rosenthal/Jöhri (eds.), *Handkommentar zum Datenschutzgesetz*, Zurich/Basel/Geneva 2008, Art. 328b OR N 38 and N 39.

³¹ *Ibid*, Art. 328b OR N 39.

³² *Ibid*, Art. 328b OR N 27 and N 40.

³³ See *ibid*, Art. 328b OR N 16, with regard to Art. 13 para. 2 let. a FADP.



(Art. 6 para. 2 let. d FADP). According to Art. 17 para. 1 let. c Revised FADP such disclosure abroad is allowed if it is “necessary” in order to safeguard an overriding public interest.

Art. 6 para. 2 let. d FADP concerns individual cases and does not justify the systematic and regular disclosure of data. The FDPIC understands that SEC requests are not regular or predictable, even though it is not excluded that large SEC regulated Swiss firms might receive several requests.

The existence of an overriding public interest must be proven under the specific circumstances. A purely hypothetical interest is not sufficient³⁴. Examples of overriding public interests include security as well as combating of fraud and money laundering. In Swiss doctrine, an overriding public interest is also considered possible in the event that a company is required by foreign law to disclose business records, for example in the context of supervision by a foreign regulatory authority³⁵. Furthermore, with Art. 42c para. 1 FINMASA, the legislator has, in principle, advocated direct transmissions to the SEC. The FDPIC therefore assumes that a transfer of personal data to the SEC is, in principle, justified by an overriding public interest. It can be based on Art. 6 para. 2 let. d FADP provided that, in the individual case, there are not any overweighing interests of the data subject that do not allow the disclosure.

With regard to client data, the FINMA considers the FDPIC’s approach to be compatible with the special protection of client confidentiality under Art. 43 para. 3bis FINMASA – the so called “private banking carve out”. This special protection of client confidentiality is tailored to on-site inspections and has no implication on cross-border transfers of client data under Art. 42c FINMASA. Furthermore, the FDPIC expressly leaves open how a disclosure of personal data that is protected by secrets under criminal law (in particular bank-client confidentiality) can be justified under criminal law, i.e. whether a consent is necessary or whether a disclosure can be justified otherwise. If criminal law requires consent, personal data may not be transferred to the SEC without such consent (see above 1.1 and 2.4.3).

2.4.6 Conclusion regarding Art. 6 para. 2 FADP

The FDPIC generally welcomes efforts to create a transfer tool in the sense of Art. 6 para. 2 let. a FADP as such tools can provide adequate data protection and create legal certainty.

He is, however, of the opinion that – from the perspective of data protection – a cross-border transfer of data to the SEC can be justified either by contract (Art. 6 para. 2 let. c FADP; see above 2.4.3 and 2.4.4) or by an overriding public interest (Art. 6 para. 2 let. d FADP; see above 2.4.5), provided that, in the individual case, there are not any overweighing interests of the data subject that do not allow for the disclosure. It is the duty and responsibility of the relevant Swiss firm to analyze whether there could be such overweighing interests of the data subject.

A data transfer to the SEC can also be justified by the consent of the data subject (Art. 6 para. 2 let. b FADP; see above 2.4.2). Provided that the data subject has been adequately informed, consent can be given by way of a single declaration of consent but, in principle, also by accepting general terms and conditions. A given consent can, however, be revoked at any time. In case data processing has been accepted by general terms and conditions and is later on revoked, the contract between the Swiss firm and its customer must be terminated as the record-keeping, reporting and inspection obligations provided by U.S. law are preconditions for rendering the relevant services. Once the contract is terminated, consent can no longer serve as a legal basis for record keeping or a disclosure of data to the SEC.

³⁴ See also Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz dated 15 September 2017, Swiss Federal Gazette 2017 p. 6941 ff., p. 7042.

³⁵ See ROSENTHAL, in: Rosenthal/Jöhri (eds.), Handkommentar zum Datenschutzgesetz, Zurich/Basel/Geneva 2008, Art. 13 N 31.



The FDPIC expressly leaves open how in cases of personal data protected by other Swiss laws a disclosure to the SEC can be justified. In particular, it must be left open under which conditions criminal law allows the transfer of personal data covered by the protection of secrets under criminal law. If criminal law requires consent, personal data may not be transferred to the SEC without such consent.

2.5 Data Protection Principles

2.5.1 General Comments

Even if a cross-border data transfer is compatible with Art. 6 FADP, a data processor must always observe the fundamental data protection principles mentioned in Art. 4, 5 and 7 FADP; otherwise the transfer is contrary to data protection.

Data processing must be proportionate (see Art. 4 para. 2 FADP). This means that a data processor may only disclose that data to the SEC that is suitable and necessary to achieve the intended purpose; furthermore, the data processing must be bearable for the data subject, both in terms of its purpose and its means. A violation of the principle of proportionality can be avoided by blackening data.

Another important principle is that the collection of personal data must be evident to the data subject (see Art. 4 para. 4 FADP). Under the Revised FADP, it does no longer suffice that the collection of data is evident to the data subject; rather the controller is obliged to inform the data subject appropriately about the collection of personal data (see Art. 19 para. 1 Revised FADP). The principle of evidence in Art. 4 para. 4 FADP as well as the obligation to inform in Art. 19 Revised FADP only apply if data are collected, but not if they are processed in another way. However, Art. 4 para. 2 FADP as well as Art. 6 para. 2 Revised FADP state that data processing must be carried out in good faith, which can mean that in certain situations not only the collection of personal data but also other forms of data processing must be made transparent (see full details below 2.5.2 ss.).

According to Art. 5 FADP anyone who processes personal data must make certain that it is correct. Moreover, personal data must be protected against unauthorized processing through adequate technical and organizational measures (Art. 7 para. 1 FADP).

2.5.2 Evidence of the Collection of Personal Data

According to Art. 4 para. 4 FADP, the collection of personal data and in particular the purpose of its processing must be evident to the data subject. The decisive factor is whether a (fictitious) average addressee or customer can recognize on the basis of the specific circumstances in the individual case that data is being collected, from whom and for what purpose, and to whom they are forwarded³⁶.

With regard to the point in time at which the data collection must be evident, it must, in principle, be evident at the time the data collection occurs; at the very least, it must be possible to foresee the exact time at which certain data will be collected. If, however, it is not reasonable for the data processor to indicate the exact point in time of the acquisition (namely because this would cause a great deal of effort), the later collection of data can be made evident in advance by corresponding general references or contractual provisions. Yet the more sensitive the personal data in question, the more likely it is that the data processor can be expected to make it evident at the time of the collection³⁷.

The Swiss firms subject to supervision by the SEC collect data at the beginning or in the course of the contractual relationship with their customer. The collection of the data and the purpose of its pro-

³⁶ Bundesamt für Justiz, Bundesgesetz über den Datenschutz, Änderung vom 24. März 2006: Häufig gestellte Fragen zur Umsetzung bei der Datenbearbeitung durch Private, 30.11.2007 (available under: [Datenschutz \(admin.ch\)](http://Datenschutz.admin.ch)), p. 2.

³⁷ Ibid, p. 2.



cessing – also a possible disclosure to the SEC – is in general made evident by corresponding contractual provisions. The question is whether also the processing of personal data in the case of a specific request by the SEC (i.e. the preparing, compiling and the intended disclosure of the data) must be made transparent. It can be argued that, at the time of a request by the SEC, the supervised Swiss firm is already in possession of the relevant data, which means that there is generally no collection of data and Art. 4 para. 4 FADP consequently does not apply. On the other hand, according to Art. 4 para. 2 FADP data processing must be carried out in good faith. This provision is likely to contain a general obligation to inform the data subjects about the processing of their data whenever this is necessary in view of the circumstances and based on a loyal and trustworthy conduct³⁸. However, if the SEC requests personal data the collection of which has taken place in an earlier stage and in compliance with Art. 4 para. 4 FADP, Art. 4 para. 2 FADP generally does not oblige the supervised Swiss firm to inform the data subject that these data are now actually processed due to a request by the SEC, even if it is sensitive personal data³⁹ or personality profiles⁴⁰. Where the data processor wants to obtain the consent of the data subject for a specific data transfer, Art. 4 para. 5 FADP provides that data subject must be informed of the intended data transfer in an adequate way (see above 2.4.2).

The Revised FADP aims at strengthening the evidence of the collection of personal data. According to Art. 19 para. 1 Revised FADP, the controller informs the data subject appropriately about the collection of personal data. At the time of collection, the controller shall provide to the data subject all information that is required in order for the data subject to assert his rights according to this Act and to ensure transparent processing of data. He shall, if applicable, also inform about the recipients or the categories of recipients to which personal data is disclosed (Art. 19 para. 2 let. c FADP), and if personal data is disclosed abroad, the controller informs the data subject of the name of the State or international body and, as the case may be, the safeguards according to Art. 16 para. 2 or the applicability of one of the exceptions provided for in Art. 17 (Art. 19 para. 4 FADP). However, Art. 19 Revised FADP regulates – as Art. 4 para. 4 FADP – but the information on data collection and does not oblige to inform about every form of data processing. Also the Revised FADP states that data processing must be carried out in good faith (see Art. 6 para. 2 FADP), but the question whether a specific intended data transfer to the SEC must be made transparent to the data subject, can be answered in the same way as under current law.

2.6 Breach of Professional Confidentiality

The question is whether a Swiss firm employee who transfers personal data to the SEC can be liable to prosecution under the FADP or the Revised FADP. According to Art. 35 para. 1 FADP, anyone who without authorization willfully discloses confidential sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine. The same penalties apply to anyone who without authorization willfully discloses confidential sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person (Art. 35 para. 2 FADP).

Art. 35 FADP only applies with regard to sensitive personal data or personality profiles. Sensitive data is data on 1. religious, ideological, political or trade union-related views or activities, 2. health, the intimate sphere or the racial origin, 3. social security measures or 4. administrative or criminal proceedings and sanctions (see Art. 3 let. c FADP). Other personal data such as e.g. financial data are not covered by this provision. The scope of application of Art. 35 FADP is therefore narrower than that of Art. 74 Swiss Federal Act on Banks and Savings Banks of 8. November 1934 (CC 952.0) which pro-

³⁸ EPINEY/CIVITELLA/ZBINDEN, *Datenschutzrecht in der Schweiz*, *Freiburger Schriften zum Europarecht* Nr. 10, 2009 (available under: [Microsoft Word - Cahier10 \(unifr.ch\)](#)), p. 23.

³⁹ Such as, e.g., data on administrative or criminal proceedings and sanctions.

⁴⁰ Art. 14 para. 1 FADP states that the controller of the data file is obliged to inform the data subject of the collection of sensitive personal data or personality profiles. This provision does not apply where there is no collection of such data, but another form of data processing.



protects bank-client confidentiality. A personality profile is a collection of data that permits an assessment of essential characteristics of the personality of a natural person (see Art. 3 let. d FADP).

According to Art. 35 FADP, only the disclosure of confidential data is punishable. Data is confidential in the sense of this provision if it is neither in the public domain nor generally accessible, the person concerned wants to keep the data confidential, and his or her interest in secrecy is an objectively legitimate one⁴¹. The disclosure must be unauthorized. In any case, this is not the case if the disclosure complies with data protection requirements⁴². Furthermore, the data must be disclosed willfully.

In view of the limited scope of application of Art. 35 FADP, the FDPIC expects that employees of Swiss firms that transfer data to the SEC are only exceptionally liable to prosecution.

Under the Revised FADP, a person shall be liable on complaint to a fine of up to 250'000 Swiss Francs if he willfully discloses confidential personal data of which he has gained knowledge while exercising his profession which requires the knowledge of such data (Art. 62 para. 1 Revised FADP). The same penalty applies to anyone who willfully discloses confidential personal data of which he has gained knowledge in the course of his activities for a person bound by a confidentiality obligation or in the course of training with such a person (Art. 62 para. 2 Revised FADP).

The Revised FADP extends the protection of secrecy to all types of personal data. Again, the decisive factor is that the data is confidential.

It cannot be excluded that a firm employee will cite this provision as a reason not to transfer personal data to the SEC. However, the FDPIC assumes that a disclosure of data that is compatible with the Revised FADP is not punishable. Furthermore, the data must be disclosed willfully.

2.7 Conclusions

The SEC would like to know whether and – if yes – under which conditions – Swiss data protection law allows Swiss-domiciled entities registered with the SEC to transfer personal data to the SEC in the course of an examination process conducted by this authority.

The U.S. legislation does not guarantee an adequate protection of the privacy as required by the FADP. A transfer of personal data to the SEC must therefore be justified under Art. 6 para. 2 FADP. The FDPIC generally welcomes efforts to create a transfer tool in the sense of Art. 6 para. 2 let. a FADP. He is, however, of the opinion that – from the perspective of data protection – a disclosure of data to the SEC can, in principle, be justified either by the consent of the data subject (Art. 6 para. 2 let. b), by contract (Art. 6 para. 2 let. c) or by an overriding public interest (Art. 6 para. 2 let. d FADP) (see above 2.4.6, with further references).

The FDPIC expressly leaves open how in cases of personal data protected by other Swiss laws a disclosure to the SEC can be justified. In particular, it must be left open under which conditions criminal law allows the transfer of data covered by the protection of secrets under criminal law. If criminal law requires consent, then personal data may not be transferred to the SEC without such consent.

Even if a cross border data transfer is compatible with Art. 6 FADP, a data processor must always observe the fundamental data protection principles mentioned in Art. 4, 5 and 7 FADP; otherwise the transfer is contrary to data protection. According to Art. 4 para. 4 FADP, the collection of personal data and in particular the purpose of its processing must be evident to the data subject. The collection of the data and the purpose of its processing – also a possible disclosure to the SEC – is, in general,

⁴¹ See Botschaft zum Bundesgesetz über den Datenschutz (DSG) dated 23 March 1988, Swiss Federal Gazette 1988 II p. 413 ss., p. 485.

⁴² ROSENTHAL, in: Rosenthal/Jöhri (eds.), Handkommentar zum Datenschutzgesetz, Zurich/Basel/Geneva 2008, Art. 35 N 14.



made evident by corresponding contractual provisions. If the SEC requests personal data the collection of which has taken place in an earlier stage and in compliance with Art. 4 para. 4 FADP, the supervised Swiss firm is generally not obliged to inform the data subject that these data are now actually processed due to a request by the SEC, even if it is sensitive personal data or personality profiles. In the view of the FDPIC, the legal situation is the same under the Revised FADP (see above 2.5).

The question is whether a Swiss firm employee who transfers personal data to the SEC can be liable to prosecution under the FADP or the Revised FADP for a breach of professional confidentiality. In view of the limited scope of application of Art. 35 FADP, the FDPIC expects that employees of Swiss firms that transfer data to the SEC are only exceptionally liable to prosecution under the FADP. Under the Revised FADP, which extends the protection of secrecy to all types of personal data, it cannot be excluded that a firm employee will cite Art. 62 Revised FADP as a reason not to transfer personal data to the SEC. However, the FDPIC assumes that a disclosure of data that is compatible with the Revised FADP is not punishable. Furthermore, the data must be disclosed willfully (see above 2.6).

The Commissioner:



Adrian Lobsiger